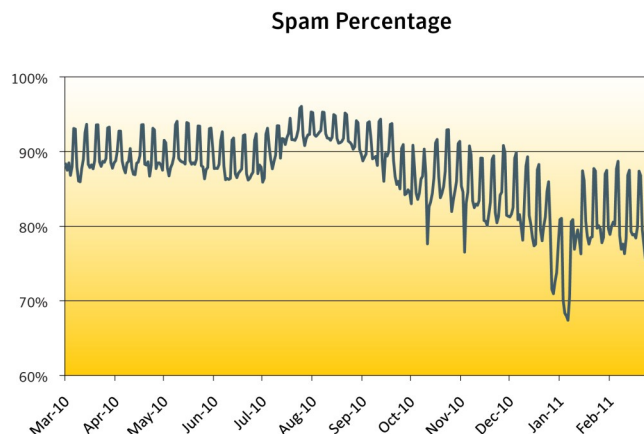




In the economic world, the media uses the acronym “BRIC” (Brazil, Russia, India, and China) as emerging market leaders. In this month’s State of Spam & Phishing report, we take a look at whether those countries are also emerging market leaders of spam. Has spam coming from that bloc of countries increased or decreased over the last year? Have any of the countries in the bloc gained or lost spam market share?



As forecasted in the last month’s report, average daily spam volume did increase for the first time since August 2010. The average daily spam volume increased 8.7 percent in February month-over-month. Overall, spam made up 80.65 percent of all messages in February, compared with 79.55 percent in January.

The overall phishing increased by 38.56 percent this month. There was significant increase in some of the sectors of phishing mostly in automated toolkit and unique domains. Phishing websites created by automated toolkits increased by about 50.33 percent. Unique URLs increased by 33.73 percent, and phishing websites with IP domains (for e.g. domains like <http://255.255.255.255>) decreased by about 47.22 percent. Webhosting services comprised 13 percent of all phishing - an increase of 38.97 percent from the previous month. The number of non-English phishing sites saw a significant increase by 76.51 percent. Among non-English phishing sites, Portuguese, French, and Spanish were the highest in February.

The following trends are highlighted in the March 2011 report:

- Examining “BRIC” for Spam
- 3D Secure Passwords for Recharging Mobile Airtime
- Mass Phishing on Credit Card Services Brand Using Fake SSL
- February 2011: Spam Subject Line Analysis

**Dylan Morss**  
Executive Editor  
Antispam Engineering

**David Cowings**  
Executive Editor  
Security Response

**Eric Park**  
Editor  
Antispam Engineering

**Mathew Maniyara**  
Editor  
Security Response

**Sagar Desai**  
PR contact  
[sagar\\_desai@symantec.com](mailto:sagar_desai@symantec.com)

### Metrics Digest

#### Global Spam Categories

Category Name	February	January	Change (% points)
Adult	<1%	1%	-1
Financial	5%	6%	-1
Fraud	4%	4%	No change
Health	6%	5%	+1
Internet	50%	47%	+3
Leisure	8%	13%	-5
419 spam	11%	6%	+5
Political	<1%	<1%	No change
Products	12%	14%	-2
scams	3%	3%	No change

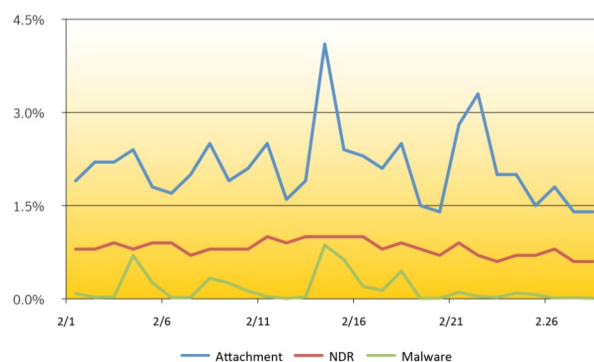
#### Spam URL TLD Distribution

TLD	February	January	Change (% points)
com	56.9%	66.8%	-9.9
ru	18.1%	11.1%	+7.0
info	9.8%	4.5%	+5.3
net	3.9%	Not listed	N/A

#### Average Spam Message Size

Message Size	February	January	Change (% points)
0-2kb	1.81%	2.99%	-1.18
2kb-5kb	72.32%	66.52%	+5.80
5kb-10kb	16.10%	21.31%	-5.21
10kb+	9.77%	9.18%	+0.59

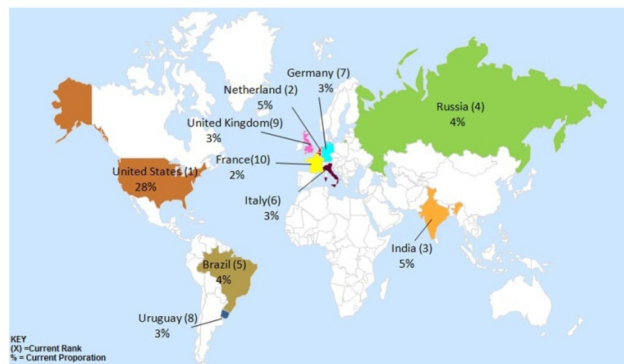
#### Spam Attack Vectors





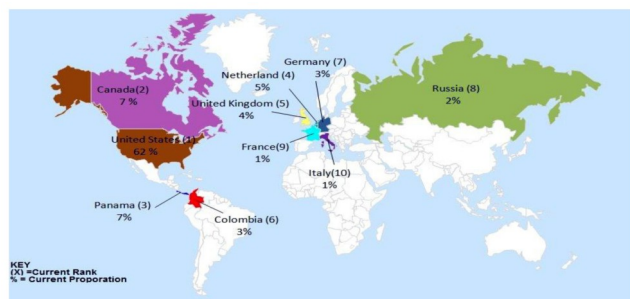
### Metrics Digest

#### Spam Regions of Origin



Country	February	January	Change (% points)
United States	28%	29%	-1
Netherlands	5%	6%	-1
India	5%	5%	No change
Russia	4%	5%	-1
Brazil	4%	5%	-1
Italy	3%	2%	+1
Germany	3%	3%	No change
Uruguay	3%	3%	No change
United Kingdom	3%	3%	No change
France	2%	Not listed	N/A

#### Geo-Location of Phishing Lures



Country	February	January	Change (% points)
United States	62%	52%	+10
Canada	7%	10%	-3
Panama	7%	Not listed	N/A
Netherlands	5%	Not listed	N/A
United Kingdom	4%	4%	No Change
Colombia	3%	Not listed	N/A
Germany	3%	6%	-3
Russia	2%	5%	-3
France	1%	Not listed	N/A
Italy	1%	3%	-2

#### Geo-Location of Phishing Hosts

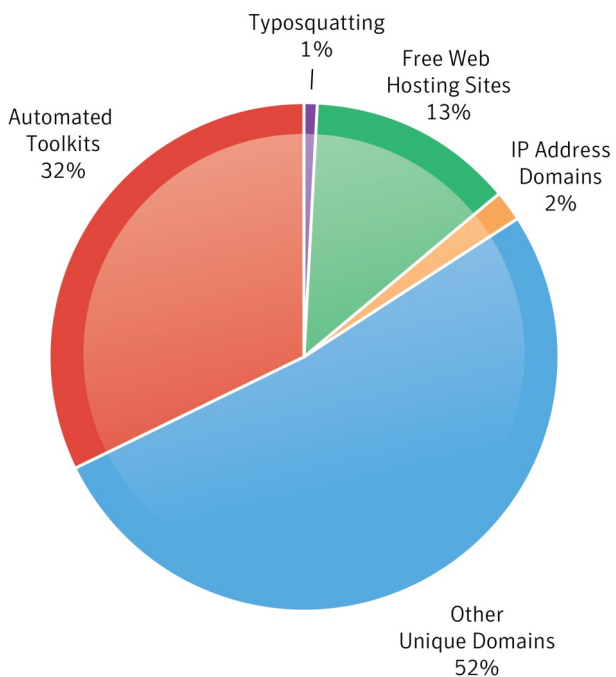


Country	February	January	Change (% points)
United States	52%	49%	+3
Germany	6%	8%	-2
United Kingdom	5%	5%	No Change
Russia	4%	4%	No Change
Brazil	3%	2%	+1
France	2%	Not listed	N/A
Canada	2%	10%	-8
Netherlands	2%	Not listed	N/A
Italy	2%	2%	No Change
South Korea	1%	Not listed	N/A

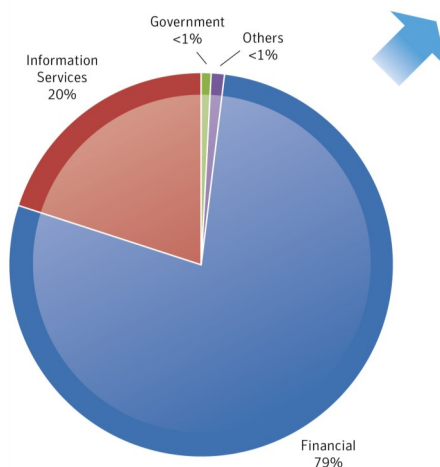
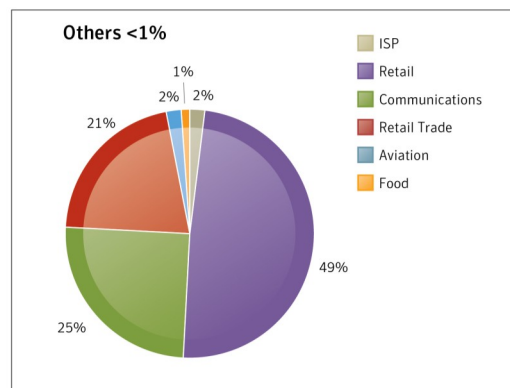
### Metrics Digest

#### Phishing Tactic Distribution

#### Overall Statistics



#### Phishing Target Sectors

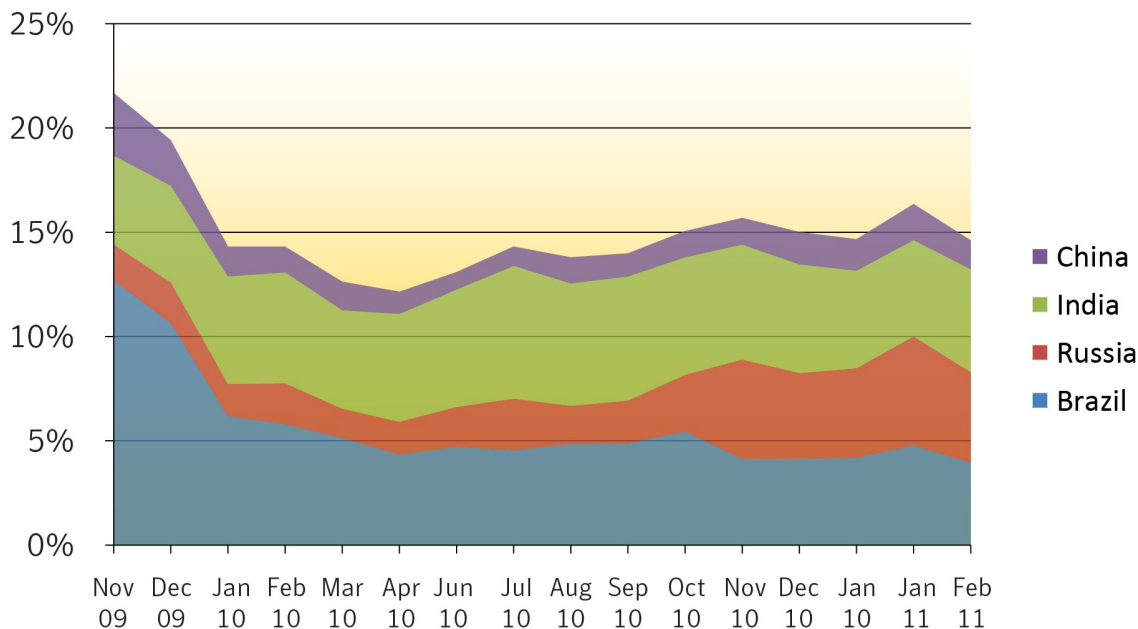




### Examining “BRIC” for Spam

We all know that “BRIC” countries (Brazil, Russia, India, and China) are the leaders of emerging market world. These countries have shown tremendous economic growth recently, and in turn have seen fast growth in broadband Internet. This growth in broadband use makes these countries vulnerable to botnets, a web of compromised computers.

So we asked the question: where are they in terms of global spam output?

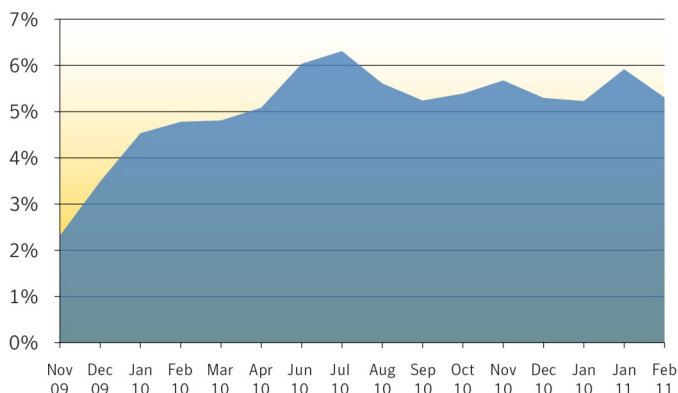


The above chart, which shows spam origin percentage by each country, highlights three major trends:

- As a whole, BRIC’s spam market share declined over the last 15 months.
- Brazil made the most nominal improvement.
- Russia, on the other hand, gained spam market share.

Over the last 15 months, EMEA has ranked consistently as the top region in global spam output. While a number of countries in EMEA region remained in the top ranking throughout the time period, one country stood out from the rest in gaining spam market share.

Netherlands, which only sent 2.3 percent of global spam in November 2009, saw its spam output increase to 5.3 percent in February 2011. The figure was actually higher in June 2010, coming in at 6.3 percent.







### 3D Secure Passwords for Recharging Mobile Airtime

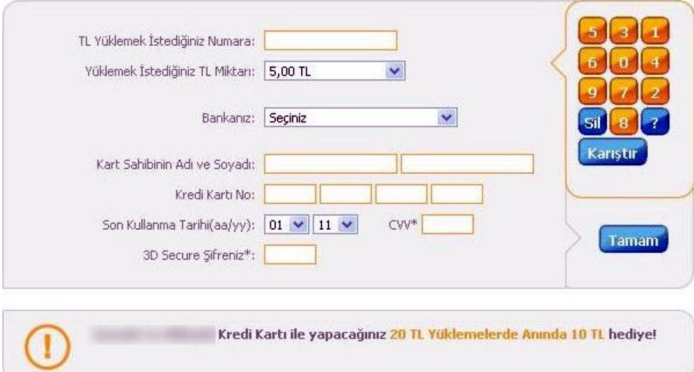
Phishers are known for developing different strategies with the motive of duping users into believing that the phishing site is authentic and secure. Phishing sites are now seen asking for a 3D secure number.

What is 3D secure number?

A 3D secure number is a password that is only known to the bank and the buyer. In other words, during an online transaction, the merchant in question does not know this number. This number is essentially an additional password given separately to card holders specifically for the safety of online transactions.

Many online transactions typically involve the use of credit/debit card numbers and the number on the back of the card. If anyone happens to see the card and copies or writes down these numbers found on the card, the card holder would be at risk of having his or her money stolen in online transactions. The use of a 3D secure password prevents such a risk, as it is a number not present anywhere on the card. The fact that the card numbers are entered by the owner of the card helps in authenticating.

A 3D secure number reduces the risk in a situation where the card numbers are copied by other people. However, if the 3D secure number itself is given away by the user to a phishing site, the user's money would still be at risk. Phishers are well aware of this and so prompt users to enter their 3D secure number along with other card details in phishing sites.



Recently, one such example was observed where the phishing site prompted the user for credit card details and their 3D secure number for an online transaction. The bait was mobile phone airtime purchased online. The phishing site targeted customers in Turkey and the phishing pages were in Turkish. Also, the credit card details requested were of banks based in Turkey. The required information was the mobile phone number, amount of mobile phone airtime to be recharged, name of the bank, card holder's name, credit card number, expiration date, CVV, and 3D secure password. To increase the appeal, the phishing page offered customers of two particular banks gifts worth \$10 for every \$20 purchased. Upon entering the information, the user was redirected to a page on the phishing site that asked for more user information.



### 3D Secure Passwords for Recharging Mobile Airtime (continued)

- İşlem Bilgisi -  
Yükleme yapılacak telefon numarası :  
Kartınızdan çekilecek tutar :

ÖNEMLİ NOT: Kartı Kullanıyorsanız 3d Secure Aktifleştirmeniz gerekmektedir. Lütfen [TIKLAYIN](#) formu doldurduktan sonra telefonunuza sms ile gelen şifreyi girin ve tekrar kontör yüklemeyi deneyin.

\* Bilgileri eksiksiz giriniz ve Onayla / Yükle Butonuna basınız.

Anne kızlık soyadı :

Kart Sahibinin Doğum Tarihi ( Gün/Ay/Yıl ) :  /  /

(Gerekli bilgi) Müşteri veya Hesap Numaranız  (Tüm bilgiler gereklidir.)  
(Bankanızı anyaraktaki öğrenebilirsiniz.)

Kart Şifreniz :

**Onayla / Yükle**

Son bir adım kaldı! Kontörünüz hattınıza en kısa sürede yüklenmesi ve hediye 10 TL kazanmış olabilmemiz için işlemi onaylamanız gerekmektedir. İşlemi onaylamamanız veyahut bilgileri eksik girmeniz durumunda işleminiz başansız olacaktır.

3D Secure: İnternette yaptığınız alışverişlerde kredi kartınızı yetkisiz kullanıma karşı korur. Bilgileriniz yüksek şifreleme sistemiyle koruyarak bilgilerinize erişimi tamamen güvenli kılar. 3D Secure ödeme sistemi olmayan yerlerden alışveriş yaparken dikkatli olunuz.

The information asked in the second phishing page consisted of mother's maiden name, card holder's date of birth, customer or account number and password. The phishing page claimed that upon clicking the button at the bottom of the page, a password would be sent as an SMS to the user's mobile phone. The user was warned that if incomplete information was entered, the operation would be disapproved, leading to the failure of the transaction. Below this button was a message stating that 3D secure card purchases are safe for online transactions and high encryption system provides protection against unauthorized use. This statement was obviously displayed to gain the user's confidence.

The third page of the phishing site asks for the password previously claimed to have been sent to the user by SMS. The phishing page also notifies the user that the SMS may take one to five minutes to reach the user and requests that the page not be closed. Of course, this is just a ploy and the user wouldn't receive a password.

The phishing URL used IP domains (for example, domains like <http://255.255.255.255>). The phishing site was hosted on servers based in the state of Orlando, USA.

Lütfen şifrenizi giriniz

Üye İşyeri :

Tarih : 20101114

Kart Numarası : XXXX XXXX XXXX XXXX

Kişisel Güvenlik Mesajı (PAM) :

İşlem şifreniz bankanıza ait kayıtlı cep telefonunuza gönderilecektir.  
Lütfen pifb0087 referans numaralı alışveriş şifrenizi giriniz.

Cep telefonunuza gönderilen SMS şifresini ekrandaki ilgili alana yazdığınızda işbu sözleşmeyi [\(YASAL UYARI\)](#) okuyup kabul etmiş sayılacaksınız.

**Yardım** **Vazgeç** **Gönder**

" 1 ila 5 Dakika içerisinde şifreniz gönderilecektir. Lütfen bu sayfayı kapatmayınız. "



### Mass Phishing on Credit Card Services Brand Using Fake SSL

In February, Symantec observed a mass phishing attack on a popular credit card services brand. There were a large number of phishing URLs in the attack, which were all secured using Secure Socket Layer (SSL).

So what makes this phishing attack stand out from the rest?

Phishing websites that use SSL are uncommon and are typically seen in very small numbers. To create a phishing site that uses SSL, the phisher would either have to create a fake SSL certificate or attack a legitimate certificate to attain an encryption for the site. In both cases, Symantec has observed that phishing sites using SSL are less frequent. In this particular attack, there were over a hundred phishing URLs that used a fake SSL certificate. This was achieved by hosting the phishing site on one single IP address which resolved to several domain names. That is, although there were abundant URLs in the attack, they all resolved to a single IP address and contained the same webpage. The SSL certificate was an expired one, with its issue date of the year 2006 and an expiration date of 2007. The phisher's primary motive behind creating an encrypted phishing site is to help the site appear authentic and to convince users that the site is safe.

The phishing site spoofed a credit card services brand, which targeted customers of Switzerland and its phishing pages were in French. End-users were also asked to provide login credentials of a popular e-commerce brand. Hence,

phishers attempted to harvest confidential information of two brands with the same phishing attack. The phishing site was hosted on servers based in the state of California, USA.

Could not verify this certificate because it has expired.

**Issued To**  
Common Name (CN) [redacted]  
Organization (O) [redacted]  
Organizational Unit (OU) Web Hosting  
Serial Number 00

**Issued By**  
Common Name (CN) [redacted]  
Organization (O) [redacted]  
Organizational Unit (OU) Web Hosting

**Validity**  
Issued On 4/7/2006  
Expires On 4/7/2007

**Fingerprints**  
SHA1 Fingerprint [redacted]  
MD5 Fingerprint [redacted]

and mother's maiden name. The second step asks for banking data including bank name, bank ID, name of card holder, card type, card number, personal code, card expiration date, and CVV number. Upon entering the requested information, the phishing site redirects to a blank webpage. If users fell victim to the phishing site, phishers would have stolen their information for financial gain.

Service Vérifié par

# Etape 1 - Vérification de l'identité.

Nom : \*

Prénom : \*

Date de naissance : \*  --Jour--  --Mois--  --Année--

Adresse : \*

Ville : \*

Code Postal : \*

Pays : \*  -- Choix d'un pays --

Telephone : \*

Votre Email

Mot de Passe

Nom de jeune fille de votre mère : \*

# Etape 2 - Données Bancaires

Nom de la banque : \*

identifiant de banque a distance :

Nom du titulaire de la carte : \*

Type de carte : \*

Numero de carte : \*

Votre code personnel : \*

Date d'expiration : \*  --Mois--  --Année--

Cryptogramme : \*

demiers chiffres du numéro inscrit au dos de votre carte). (Il s'agit des 3 derniers chiffres du numéro inscrit au dos de votre carte).





### February 2011: Spam Subject Line Analysis

#	Total Spam: February 2011 Top Subject Lines	No of Days	Total Spam: January 2011 Top Subject Lines	No of Days
1	Find Out How You Can Start Making \$6487 a Month At HOME	12	Re:	31
2	Re:	15	Find Out How You Can Start Making \$6487 a Month At HOME	29
3	Sarah Sent You A Message	11	Marina 21y.o, I am on-line now, let's chat?	2
4	Save-On-Cialis-Viagra-And-Many-Other-Meds-NOW	9	New post	3
5	<i>Blank Subject line</i>	15	New In town	12
6	Have Great SEX And Save 80% Valentines Day Special	8	Save-On-Cialis-Viagra-And-Many-Other-Meds-NOW	15
7	Hookup 2 Night!	8	<i>Blank Subject line</i>	31
8	Guaranteed Quality of Viagra Pills, Fast delivery and Low prices.	5	New Message	15
9	Trusted Pharmacy >>> Viagra for Sale	5	RE: Date	18
10	Viagra for Sale in our FDA Approved Drugstore. Guaranteed Quality of Pills, Fast delivery and Low prices.	6	[NO SUBJECT]	6

419 spam messages are usually smaller attacks, rather than millions of messages sent with same subject line. This could explain why these attacks are not seen in the above analysis despite the fact that the category saw 5 percentage point increase month-over-month. Nevertheless, Symantec observed many 419 spam attacks which leveraged current events.

**From:** Hosni Mubarak  
**Date:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** President Hosni Mubarak

Hello Dear,


My contacting you through this medium is due to the urgency and confidentiality of this message; I want to make you an offer so that you can assist me.

I resigned as the Egyptian President on the 11th of February 2011, please go through this:

[http://www/\[REDACTED\]](http://www.[REDACTED])

I know very well that the new government will be after all the moneys with me, and as such, I don't want to lose all. I have some deposited amount of money, which I will like you to change the ownership to you and have the money moved immediately to you in your country in Cash (US\$56Million) through a high Diplomatic Service.

Once you have received this first part, I will move another to you, but I want you to assure me that you can handle this easily, as I will take care of all the documentation here and the cost here. What you are to take care of is just the delivery and handling charges once they have arrived your country.

**From:** ICC World Cup 2011 Cricket  
**Date:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** CRICKET AWARD WINNER\*  
**Attach:**  INTERNATIONAL CRICKET PROMOTION.doc (33.5 KB)

INTERNATIONAL (WORLD) CRICKET QUIZ 2011  
 UK Ltd Belgrave House 76,  
 Buckingham Palace Road,  
 London SW1W 9TQ,  
 United Kingdom.

Good Day

Kindly open

Regards,

Mr Jeral

Member,

ICC 201

United K

**From:** CHARITY  
**Date:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** Pro-Gadhafi forces fight rebels in 2 cities (AP)

My Dearest in God,

I just escaped and arrived RSA from Libya. It was not easy.  
 I have the family oil recourses for charity Kindly open the link below.

For all info, Reply now



### Checklist: Protecting your business, your employees and your customers

#### Do

- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. Deselect items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid publishing your email address on the Internet. Consider alternate options – for example, use a separate address when signing up for mailing lists, get multiple addresses for multiple purposes, or look into disposable address services.
- Using directions provided by your mail administrators report missed spam if you have an option to do so.
- Delete all spam.
- Avoid clicking on suspicious links in email or IM messages as these may be links to spoofed websites. We suggest typing web addresses directly in to the browser rather than relying upon links within your messages.
- Always be sure that your operating system is up-to-date with the latest updates, and employ a comprehensive security suite. For details on Symantec's offerings of protection visit <http://www.symantec.com>.
- Consider a reputable antispam solution to handle filtering across your entire organization such as Symantec Brightmail messaging security family of solutions.
- Keep up to date on recent spam trends by visiting the Symantec State of Spam site which is located [here](#).

#### Do Not

- Open unknown email attachments. These attachments could infect your computer.
- Reply to spam. Typically the sender's email address is forged, and replying may only result in more spam.
- Fill out forms in messages that ask for personal or financial information or passwords. A reputable company is unlikely to ask for your personal details via email. When in doubt, contact the company in question via an independent, trusted mechanism, such as a verified telephone number, or a known Internet address that you type into a new browser window (do not click or cut and paste from a link in the message).
- Buy products or services from spam messages.
- Open spam messages.
- Forward any virus warnings that you receive through email. These are often hoaxes.

\* Spam data is based on messages passing through Symantec Probe Network.

\* Phishing data is aggregated from a combination of sources including strategic partners, customers and security solutions.